

KURSBESCHREIBUNG

Check Point Advanced Troubleshooting Workshop

Zielgruppe

Dieser Workshop ist für Administratoren und Security Engineers konzipiert, die bereits einschlägige Erfahrung mit Check Point Firewalls sammeln konnten.

Voraussetzungen

Wissen im Bereich TCP/IP (Version 4).
Grundlegendes Konzept zu IP Routing (Statisches Routing), IP-Adressierung, OSI-Referenzmodell, Firewalls und Application Layer Services.
Die genannten Bereiche sind nicht Bestandteil des Workshops!
Empfohlen werden die Kenntnisse eines CCSA´s, wobei die Version unabhängig ist.

Lernziele

In diesem Workshop werden diverse Möglichkeiten angesprochen, um eine gründliche und eingehende Fehleranalyse im Check Point-Umfeld durchzuführen.
Teilweise kommen dabei Befehlssequenzen zum Einsatz, die im Verlauf einer CCSE-Ausbildung nicht angesprochen werden. Nach dem Besuchen dieses dreitägigen Workshops werden die Teilnehmer mit einem soliden Rüstzeug ausgestattet und werden in die Lage versetzt, zahlreiche Probleme selbständig zu lösen.

Inhalt

- Allgemeine Konzepte zu Fehleranalyse
  - Der interne Prozess bei der Installation einer Policy
  - Die hauptsächlichen VPN-1 Prozesse
  - Die wichtigsten Konfigurationsdateien
  - Wichtige Kommandos zur Zustandserfassung des Check Point-Systems
- FW Monitor
  - Was ist ‘fw monitor’?
  - Praktische Beispiele für detaillierte Paketfluss-Analyse mit FW MONITOR
  - Analyse des Outputs von FW MONITOR mittels WireShark
  - Weitere Beispiele aus der Praxis



- Kernel Debug in NGX
  - Paketfluss im Kernel und durch die Chain Modules
  - Debugging auf Prozess-Ebene (fwm, fwd, ...)
  - Debug Flags
  - Debugging Tipps
  - Beispiele
- NAT Debugging
  - Was ist NAT?
  - Wie kann man NAT Debugging durchführen?
  - Praktisches Beispiel anhand von Hide NAT
  - Analyse von Dynamic NAT und Port Address Translation
- VPN Troubleshooting
  - Allgemeines zu IPSec VPN
  - Phase 1: Aushandeln der IKE SA im Main Mode (Aggressive Mode)
  - Phase 2: Aushandeln der IPSec SA im Quick Mode
  - Logging von VPN Techniken zum Reinitialisieren bestehender Tunnel
    - Typisches Problem aus der Praxis: "Invalid ID Information"
    - Typisches Problem aus der Praxis: "No Proposal Chosen"
    - Typisches Problem aus der Praxis: "Payload Malformed"
  - VPN Daemon in den Debug Mode versetzen
- Clustering
  - Das Konzept von ClusterXL, Nokia VRRP und IP Clustering
  - Die verschiedenen Modi von ClusterXL (HA ,Load Sharing)
  - Diverse Szenarien mit Clustern (Hotfix-Installation, Upgrade, ...)
  - Nokia VRRP und IP Cluster im Detail
  - Fehleranalyse bei Clustern
- Performance-Optimierung mit SecureXL und CoreXL
  - Was ist SecureXL?
  - Was ist CoreXL?
  - Definition von Prozessor-Rollen in CoreXL (SND, FWD)
  - Konfiguration von Affinity der Netzwerkkarten an SNDs Analyse von Flow Templates